jamf

Verwalten und schützen Sie Ihre anfälligsten Endpoints: mobile Geräte

Wenn wir von mobilen Geräten sprechen, denken wir an Laptops, Tablets und Smartphones. Obwohl jedes Gerät in die Kategorie der mobilen Geräte fällt, konzentriert sich dieser Beitrag auf Smartphones und Tablets. Millionen von Nutzer*innen weltweit verlassen sich auf diese Geräte, um ihre täglichen Aufgaben bei der Arbeit, in der Schule und im Privatleben zu bewältigen. Diese Abhängigkeit von mobilen Geräten hat jedoch auch erhebliche Bedenken hinsichtlich der mobilen Sicherheit aufgeworfen.

Es ist möglich, Ihre mobilen Endpoints zu schützen und gleichzeitig die Compliance mit Ihrer bestehenden Mac Flotte aufrechtzuerhalten. Nach dem Lesen dieses Artikels wissen Sie, wie Sie den Schutz mobiler Geräte effektiv und effizient mit derselben erstklassigen Sicherheitslösung für Endpoints abstimmen können, mit der Ihre gesamte Flotte - Mac und mobile Geräte - sicher und die Daten geschützt sind.

Tauchen Sie ein und erfahren Sie mehr:

Stand der mobilen Sicherheit >

Landschaft für die Bereitstellung mobiler Geräte in Unternehmen >

Ganzheitlicher Ansatz für die Verwaltung und den Schutz mobiler Geräte >

Schlüssel zur Vereinheitlichung der Verwaltung und Sicherheit von Mobilgeräten und Macs >

Stand der mobilen Sicherheit

Im Zuge des technischen Fortschritts nutzen die Menschen zunehmend mobile Geräte. Diese Geräte bieten die Funktionen eines Desktop-Computers, aber in einem schlanken, leichten und energieeffizienten Design. Sie ermöglichen die ganztägige Nutzung, schnelle Netzwerkverbindungen und den Zugriff auf verschiedene Apps und Dienste von überall und jederzeit.

Aus Unternehmenssicht verringern mobile Geräte die Einschränkung des Arbeitsortes, während die Netzkonnektivität die Abhängigkeit von bestimmten Plattformen beseitigt hat, unter anderem dank des Echtzeitzugriffs auf cloudbasierte Dienste. Während die Bereitstellung firmeneigener mobiler Geräte für jeden Mitarbeiter/jede Mitarbeiterin einen Kostenfaktor darstellt, hat die weit verbreitete Nutzung mobiler Geräte für den persönlichen Gebrauch mehrere Eigentumsmodelle für Unternehmen hervorgebracht, wie firmeneigene, persönlich registrierte Geräte (COPE), Mitarbeiterwahlprogramme und Bring Your Own Device (BYOD) Initiativen. Mit BYOD profitieren Unternehmen von den Kosteneinsparungen, die dadurch entstehen, dass die Nutzer*innen ihre persönlichen Geräte für die Arbeit nutzen können. Im Gegensatz dazu können die Nutzer*innen ihre Arbeitsaufgaben über die Plattform und den Formfaktor erledigen, die sie bevorzugen.

Die zunehmende Akzeptanz und Abhängigkeit von mobilen Geräten bedeutet aber auch, dass die Sicherheit eine größere Rolle spielt. Einige der häufigsten Auswirkungen auf das Unternehmen sind:

- Zusätzliche Risiken von Datenlecks
- Unbefugter Zugriff auf private Benutzerinformationen
- Mangelnde Parität zwischen mobilen Geräten und Mac Endpoint-Sicherheit
- Schwierigkeit bei der Bewertung und Einhaltung der Vorschriften
- Kompromittierung von Geräten kann zu Datenschutzverletzungen führen

Organisationen haben oft ein falsches Gefühl der Sicherheit. Die Lücken zwischen den Sicherheitsrichtlinien, die für den Schutz von Computern entwickelt wurden, und der Wirksamkeit ihrer Durchsetzung auf mobilen Geräten können die Sicherheitslage von mobilen Geräten schwächen und die Sicherheitslage des Unternehmens insgesamt verringern. Ein anderer Aspekt ist die Komplexität, die mit der Unterstützung mehrerer Plattformen einhergeht, was sich auf die Geschwindigkeit der mobilen Bereitstellung auswirkt - sowohl bei der Bereitstellung unternehmenseigener Geräte für die Nutzer*innen als auch bei der Gewährleistung der Sicherheit von Unternehmensdaten auf privaten Geräten, die für die Arbeit genutzt werden. All dies ohne Beeinträchtigung der Privatsphäre des Nutzers/der Nutzerin oder der Benutzerfreundlichkeit seines Geräts.

Eine weitere wichtige Überlegung ist, ob Ihr Unternehmen Richtlinien hat, die die Nutzung von Mobilgeräten einschränken, die nicht unter ein BYOD-Programm fallen. Wenn Sie glauben, dass Ihr Unternehmen gegen mobile Bedrohungen immun ist, sollten Sie das unbedingt überdenken. Stellen Sie sich zunächst die Frage, ob wir die private Nutzung von Mobilgeräten erlauben.

Für die Unternehmen, die mit „Nein" antworten, lohnt es sich, eine Folgefrage zu stellen: Was ist mit Szenarien wie der Nutzung eines Tablets durch den CEO auf Reisen? Dieses Tablet, das die Kinder auch für ihre Hausaufgaben nutzen, kann so konfiguriert sein, dass es Zugriff auf private Firmen-E-Mails hat. Oder denken Sie an die Smartphones, die von Vorstandsmitgliedern und Geschäftsführern verwendet werden, um Sitzungen zu planen und vertrauliche Geschäftsvorgänge zu besprechen. Diese Geräte werden häufig für die organisatorische Kommunikation eingesetzt und können als potenzielle Angriffsflächen dienen, auch für Angriffe im Zusammenhang mit Walfangkampagnen.

Mobilitätstreiber

Das herkömmliche Konzept der Unternehmensmobilität, das sich auf die Entwicklung unserer Arbeitsweise bezieht, stand vor erheblichen Herausforderungen, die eine rasche Veränderung der Organisationsmodelle erforderlich machten. Dieser Wandel wurde durch verschiedene Faktoren vorangetrieben, darunter:

> Die Migration von Operationen zu Cloud Diensten

> Die Einführung von verteilten Arbeitsplätzen

> Die zunehmende Verbreitung von nativen mobilen Apps

Die Entwicklung und Nutzung mobiler Geschäftsapps passt sich nahtlos an die sich ständig verändernden Arbeitsumgebungen an und macht mobile Geräte zu unverzichtbaren Werkzeugen. Dies ist vor allem auf ihre Bequemlichkeit, Anpassungsfähigkeit, ihr Engagement und ihre Kosteneffizienz zurückzuführen.

Der Schwerpunkt liegt dabei auf der Bedeutung mobiler Geräte und Geschäftsapps für den modernen, globalen Arbeitsplatz:

Mobile Geräte für mehr Arbeitseffizienz:

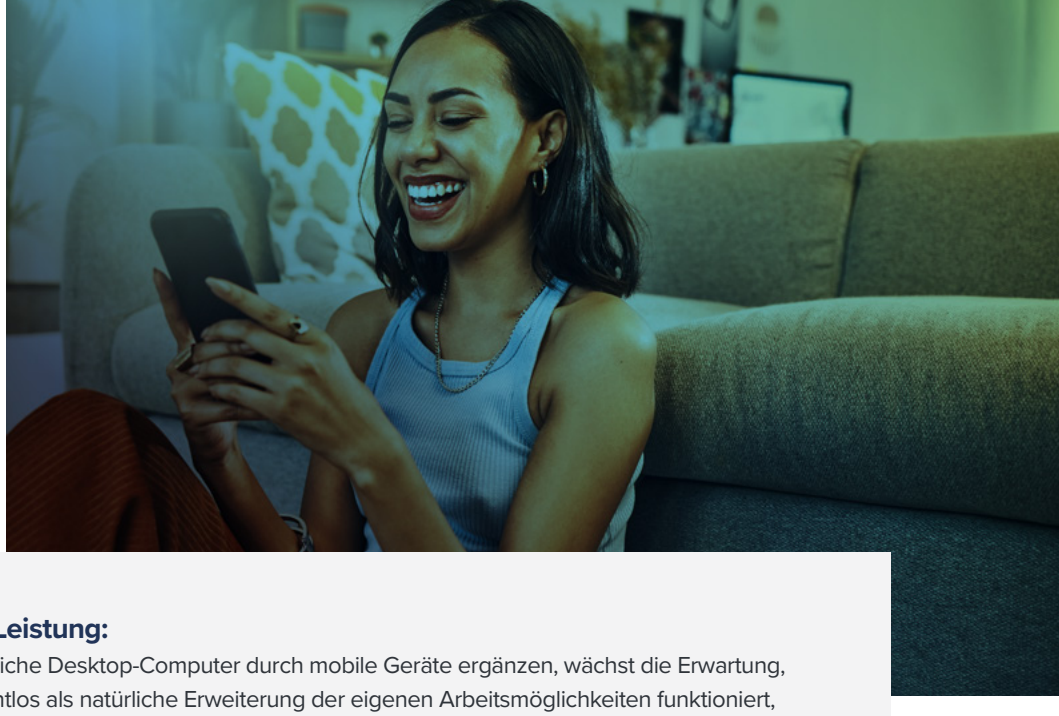
Mobile Geräte, wie z. B. Smartphones, sind zu wichtigen Arbeitsmitteln geworden. Sie ermöglichen es den Nutzer*innen, von überall aus auf Geschäftsapps zuzugreifen und sich mit Netzwerken zu verbinden, was intelligentere und effizientere Arbeitsabläufe fördert.

Beliebtheit von mobilen Geschäftsapps:

Mobile Geschäftsapps werden aufgrund ihrer nahtlosen Anpassung an dynamische Arbeitsumgebungen immer beliebter. Sie gelten aufgrund ihrer Bequemlichkeit, Personalisierung, ihres Engagements und ihrer Kosteneffizienz als unverzichtbar.

Vielseitige Arbeitsabläufe:

Mobile Geräte erleichtern die Entwicklung effektiver Arbeitsabläufe für verschiedene Arbeitsaufgaben. Benutzer*innen können auf ihren mobilen Geräten problemlos Aktivitäten wie Videokonferenzen, Enterprise Messaging, die gemeinsame Bearbeitung von Dokumenten und die Bearbeitung von Geschäfts-E-Mails durchführen.



Erwartung an die mobile Leistung:

Da viele Nutzer*innen herkömmliche Desktop-Computer durch mobile Geräte ergänzen, wächst die Erwartung, dass die mobile Technologie nahtlos als natürliche Erweiterung der eigenen Arbeitsmöglichkeiten funktioniert, und zwar sowohl effizient als auch schnell.

Innovation am Arbeitsplatz:

Mobile Geräte spielen eine entscheidende Rolle bei der Innovation am Arbeitsplatz und tragen zur Zufriedenheit, Produktivität und Bindung der Mitarbeiter*innen bei. Sie ermöglichen es Unternehmen, einfachere und effizientere Wege zu finden, um Aufgaben zu erledigen und sich an ein verändertes Arbeitsumfeld anzupassen.

Anhaltendes Wachstum von Mobilgeräten:

Mobile Geräte dominieren weiterhin den Markt, da die meisten Nutzer*innen über mobile Geräte auf das Internet zugreifen und arbeitsbezogene Aufgaben erledigen. Dies zeigt sich im kontinuierlichen Wachstum des Marktanteils von mobilen Geräten im Vergleich zum Vorjahr, wobei die „weltweite Aufteilung zwischen mobilen, Desktop- und Tablet-Nutzer*innen 58,72 %, 39,18 % und 2,1 % betrug", so Statcounter GlobalStats.

Trends zur Tele- und Hybridarbeit: Die Nachfrage nach flexiblen Arbeitsplätzen, die durch die Einführung von Remote-Arbeitslösungen im Jahr 2020 beschleunigt wird, steht im Einklang mit der weit verbreiteten Nutzung von Mobilgeräten. Die Einführung mobiler Endgeräte ist eine wichtige Voraussetzung für die Schaffung von Remote- und hybriden Arbeitsumgebungen, was durch die starke Präferenz der Mitarbeiter*innen für Remote-Arbeit belegt wird. FlexJobs hat herausgefunden, dass 97 % der befragten Arbeitnehmer*innen in irgendeiner Form eine Möglichkeit zur Fernarbeit wünschen, sei es in Form einer vollständigen Fernarbeit oder eines Hybridmodells.

Globaler Besitz von Mobilgeräten:

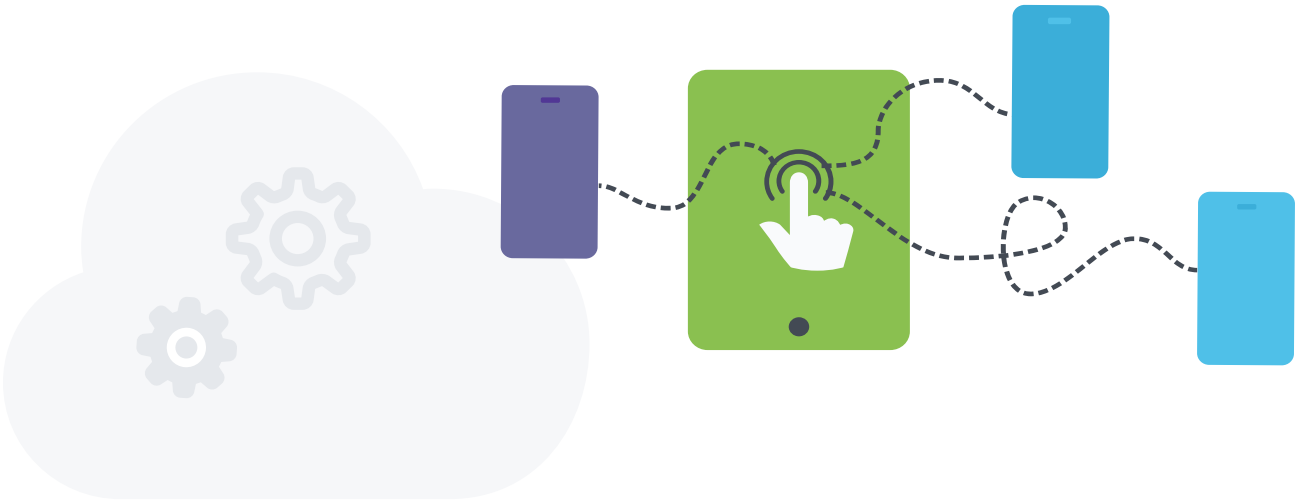
Die weite Verbreitung mobiler Geräte wird durch die Tatsache unterstrichen, dass die überwiegende Mehrheit der Weltbevölkerung Mobiltelefone besitzt, wobei Smartphones einen erheblichen Teil dieser Geräte ausmachen. Nach Angaben von Statistica werden im Jahr 2023 90,97 % der Weltbevölkerung Mobiltelefone besitzen, davon 85,88 % Smartphones.

Die Landschaft der mobilen Unternehmensbereitstellung

In der Vergangenheit haben sich Unternehmen in der Regel bewusst dafür entschieden, ihre geschäftlichen Anforderungen auf eine einzige Plattform auszurichten, bei der es sich häufig um Microsoft Windows handelte. Dazu gehörte die Beschaffung von Computern, die mit dem gewählten Betriebssystem kompatibel waren. Durch Unternehmensvereinbarungen mit Microsoft konnten Unternehmen die Bereitstellung der neuesten Windows Version so lange hinauszögern, bis sie auf den Übergang vorbereitet waren. Der Vorteil war, dass ältere Betriebssystemversionen über einen längeren Zeitraum weiter unterstützt wurden, um den Bedürfnissen dieser Organisationen gerecht zu werden.

Doch genau hier liegt die Herausforderung: Die mobile Landschaft, die traditionell als verbraucherorientiert gilt, betrachtet Betriebssystem-Patches als Aktualisierungen, die implementiert werden sollten, sobald sie verfügbar sind. Da die Benutzer*innen selbst bestimmen können, wann und wie schnell nach der Veröffentlichung von Aktualisierungen diese installiert werden, hat sich dies in den Unternehmen als Hindernis für die Akzeptanz erwiesen:

- **Vielfältige Auswahl an mobilen Betriebssystemen**
- **Fragmentierung zwischen unterstützten Versionen innerhalb jedes Betriebssystems**
- **Entwicklung von Bereitstellungsmethoden für verschiedene Betriebssysteme**
- **Unterschiedliche Unterstützung führt zu verzögerten Upgrades**
- **Unterschiedliche Unterstützung für Unternehmensanwendungen in verschiedenen Betriebssystemversionen**
- **Unterschiedliche Aktualisierungszeitpläne und Funktionsunterstützung durch die Entwickler*innen**
- **Unterschiedliche Eigentumsmodelle mit Auswirkungen auf die Verwaltung (z. B. BYOD vs. COPE)**
- **Unterstützte vs. nicht unterstützte Funktionen in MDM-Lösungen (nativ vs. nicht-nativ für Frameworks)**
- **Unterschiedliche Sicherheitsstufen für verschiedene Betriebssysteme**
- **Begrenzte richtlinienbasierte Durchsetzung von Compliance-Anforderungen**



Zunehmende Besorgnis

Wir haben die Sicherheitsbedenken im Zusammenhang mit der raschen Zunahme der Nutzung mobiler Geräte in Unternehmen bereits angesprochen. In diesem Abschnitt befassen wir uns eingehender mit den Bedrohungen, die auf mobile Geräte abzielen, und den Risiken, die mit ihrer Nutzung verbunden sind. Außerdem werden wir uns mit häufigen Missverständnissen über die Sicherheit mobiler Geräte am Arbeitsplatz befassen.

Das erste Problem ergibt sich aus der mobilen Natur dieser Geräte, die aus mehreren Gründen ein attraktives Ziel für Bedrohungsakteur*innen sind:

1

Wertvolle Datenspeicherung:
Mobile Geräte enthalten eine Fülle von persönlichen, geschäftlichen und gesetzlich geregelten Daten wie PHI (persönliche Gesundheitsinformationen) - sogar nicht gesetzlich geregelte, aber sensible Daten wie PII (persönlich identifizierbare Informationen). Bedrohungsakteur*innen können diese Informationen für verschiedene Zwecke ausnutzen und möglicherweise Angriffe auf Benutzer*innen oder Organisationen starten. Es ist wichtig, diese Daten auf mehreren Ebenen zu schützen, um sicherzustellen, dass nur autorisierte Benutzer*innen Zugriff haben.

2

Anfällig für Verlust oder Diebstahl:
Die Mobilität mobiler Geräte ermöglicht es den Nutzer*innen, von verschiedenen Orten aus zu arbeiten, erhöht aber auch das Risiko des Diebstahls oder des Verlegens. Bedrohungsakteur*innen können die Gelegenheit nutzen, um Geräte zu stehlen, was eine direkte Bedrohung für die Datensicherheit darstellt. Selbst ein kurzer unbeaufsichtigter Zugriff auf ein Gerät kann es gefährden oder anfällig für künftige Angriffe machen.

3

Missverständnisse über Sicherheit:
Einige glauben, dass mehr als verschiedene Sicherheitslösungen erforderlich sind. Die sich schnell entwickelnde mobile Bedrohungslandschaft erfordert jedoch eine native Unterstützung für Endpoint-Frameworks. Der Rückgriff auf Lösungen, die diese Unterstützung nicht bieten, kann die Anfälligkeit erhöhen, da Angriffsvektoren in nicht unterstützten Funktionen und Merkmalen offen gelassen werden.

Übermäßig geschützt oder zu wenig verwaltet: das Gleichgewicht finden

Ausgewogenheit ist ein wichtiges Konzept im Zusammenhang mit der Mobiltechnologie und dem breiteren Bereich der Sicherheit und Verwaltung. Obwohl dies oft als ein Tauziehen zwischen IT- und Sicherheitsteams dargestellt wird, ist es in Wirklichkeit so, dass es nicht ausreicht, sich nur auf eine MDM-Lösung zu verlassen. Unternehmen sollten Verwaltung und Sicherheit als integrale Bestandteile betrachten, um eine wirklich effektive mobile Sicherheitslösung zu schaffen.

Die Herausforderung besteht darin, das richtige Gleichgewicht zu finden. Eine übermäßige Absicherung von Geräten durch einen Flickenteppich von Lösungen kann zu einer minderwertigen Benutzererfahrung führen, während eine Vernachlässigung der mobilen Sicherheit wertvolle Vermögenswerte gefährden kann. Es geht nicht darum, das eine dem anderen vorzuziehen, sondern darum, das Gleichgewicht zwischen Verwaltung und Sicherheit als Leitprinzip für eine wirksame und anpassungsfähige mobile Sicherheit zu begreifen.

Ausgaben	Übermäßiger Schutz	Unterverwalten
Beeinträchtigte Leistung		✔
Benutzerfreundlichkeit		✔
Schatten-IT (Bedenken hinsichtlich des Datenschutzes können Mitarbeiter*innen dazu bewegen, persönliche Geräte zu verwenden)		✔
Umgehung von Sicherheitsmaßnahmen des Unternehmens		✔
Untergräbt das Potenzial des mobilen Arbeitsplatzes		✔
Einhaltung der rechtlichen Compliance	✔	
Entschärft sich entwickelnde mobile Bedrohungen	✔	
Trennung der Geschäftsdaten von den persönlichen Daten in einem separaten, verschlüsselten Volumen	✔	
Sicherstellen, dass die Patches in regelmäßigen Abständen korrigiert werden	✔	
Optimiert die Bereitstellung von mobilen Endpoints	✔	
Verhindert unbefugten Zugriff auf Unternehmensressourcen	✔	
Angemessener Schutz der Privatsphäre der Benutzer*innen bei gleichzeitigem Schutz der Unternehmensressourcen		✔

Der ganzheitliche Ansatz: Lehren aus dem Mac Paradigma

Wenn Ihr Unternehmen Mac Computer absichert, warum sollte es dann nicht auch mobile Geräte absichern?

Unabhängig von Ihrer Branche oder Ihrem regionalen Standort haben Unternehmen auf der ganzen Welt Apple Geräte für die Arbeit eingesetzt und tun dies auch weiterhin. Bedenken Sie, dass der Jahresumsatz von Apple vor weniger als zwei Jahren laut Apple Statistiken noch 365,8 Milliarden Dollar betrug! Der prozentuale Anteil dieses Umsatzes, der durch den Verkauf von iPhone (51,9 %) und iPad (8,8 %) zusammen erzielt wurde, betrug 60,7 %. Die Apple Watch allein verkaufte mehr als iPad und Mac (9,8 %) und trug 10,4 % zum Gesamtumsatz bei.

Es besteht eine deutliche Nachfrage nach mobilen Geräten mit verschiedenen Betriebssystemen, darunter iOS, iPadOS, Windows, Android und ChromeOS.

Es ist erwähnenswert, dass die Strategien, die zum Schutz dieser zugrunde liegenden Betriebssysteme eingesetzt werden, mehr Ähnlichkeiten als Unterschiede aufweisen. Das bedeutet nicht, dass sie identisch sind, aber es lassen sich einige Parallelen ziehen. Die viel gepriesene Apple Benutzerfreundlichkeit und die Betonung der Ausgewogenheit von Sicherheit, Verwaltung und Datenschutz lassen sich beispielsweise direkt und sinnvoll auf die mobile Sicherheit anwenden. Dieser Ansatz ermöglicht eine umfassende Strategie zum Schutz aller Endpoints in Ihrer Flotte vor potenziellen Bedrohungen.

Die Grundlage für effektive Mac Sicherheit beginnt bei Apple selbst. Das liegt an der Art und Weise, wie sie ihre Hard- und Software entwickeln, indem sie Komponenten nahtlos integrieren, bei denen Sicherheit und Datenschutz von Anfang an integriert sind und nicht erst im Nachhinein oder separat hinzugefügt werden. Ein Schlüsselelement, das diese Grundlage stärkt, ist die Verwendung der nativen Frameworks von Apple. Entwickler*innen müssen sich an diese Rahmenbedingungen halten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten, wenn Nutzer*innen mit ihren Geräten arbeiten.

Bei der Entwicklung dieser Frameworks wurde viel Wert darauf gelegt, dass sie mit den Grundprinzipien von Apple übereinstimmen, wie z. B. Benutzerfreundlichkeit und Einfachheit. Interessanterweise gehen diese Grundsätze auch auf einen häufig geäußerten Kritikpunkt an Sicherheitsmaßnahmen ein, nämlich dass strenge Sicherheitsbeschränkungen die Benutzer*innen daran hindern, effizient und komfortabel zu arbeiten. Auch hier geht es darum, ein Gleichgewicht zu finden.

Im Folgenden finden Sie einige Strategien, die Unternehmen bei der Umstellung auf ein mobiles Sicherheitskonzept helfen können, bei dem die Privatsphäre der Benutzer*innen im Vordergrund steht und gleichzeitig die Sicherheitsmaßnahmen verbessert werden:

1. Priorisieren Sie benutzerfreundliche Sicherheits-Workflows: Integrieren Sie Benutzerfreundlichkeit und Einfachheit in die Sicherheitsprozesse. Davon profitieren sowohl die Nutzer*innen als auch die Teams, die für die Verwaltung und den Schutz mobiler Geräte zuständig sind.

2. Umstellung auf datenzentrierte Sicherheit: Anstatt sich ausschließlich auf die Gerätesicherheit zu konzentrieren, sollten Sie sich auf die Datensicherheit konzentrieren. Der Schutz von Geräten ist zwar wichtig, aber sie sind austauschbar. Sensible Daten hingegen müssen immer geschützt werden.

3. Akzeptieren Sie unterschiedliche Eigentumsmodelle: Seien Sie offen für unterschiedliche Eigentumsmodelle und passen Sie die Sicherheitsmaßnahmen so an, dass sie die Unternehmensressourcen schützen, die von verschiedenen Benutzergeräten aus zugänglich sind. Das Ignorieren bestimmter Geräte kann zu Schwachstellen in Ihrer gesamten Sicherheitsstrategie führen.

4. Umfassender Datenschutz: Sorgen Sie dafür, dass die Daten in all ihren Formen sicher sind. Dazu gehört die Verschlüsselung von Datenträgern, die Trennung von geschäftlichen und persönlichen Daten und die Sicherung von Daten, die über eine beliebige Netzverbindung übertragen werden.

5. Moderne mobile Technologien einsetzen: Setzen Sie auf Technologien, die den Anforderungen moderner mobiler Geräte gerecht werden. Herkömmliche Sicherheitstools schützen oft nicht vor neuen mobilen Bedrohungen, was zu einem falschen Sicherheitsgefühl führt.

6. Split-Tunneling einführen: Erkennen Sie, dass mobile Effizienz entscheidend ist. Geschäftsdaten, die geschützt werden müssen, werden sicher weitergeleitet, während geschäftsfremde Daten, wie z. B. persönliche Informationen, die Sicherheitsprotokolle des Unternehmens umgehen können. Durch diesen Split-Tunneling-Ansatz wird die Datensicherheit aufrechterhalten und gleichzeitig die Privatsphäre der Benutzer*innen auf BYO-Geräten geschützt.

Ergebnisse der Behandlung von Mobiltelefonen wie Macs:

Welche Auswirkungen hat die zunehmende Integration von macOS und iOS auf die Zukunft der Mobil- und Endpoint-Sicherheit?

Der Vergleich von Mac, einem Desktop-Betriebssystem, mit mobilen Geräten mag zwar wie der Vergleich von Äpfeln mit Birnen erscheinen, aber Tatsache ist, dass jede neue Version von macOS und iOS eine größere Konvergenz zwischen diesen Betriebssystemen mit sich bringt. Mit jeder neuen Version wird die Frage nach der Bedeutung dieser Integration immer wichtiger.

Die wichtigere Frage ist jedoch, wie Unternehmen diese tiefere Integration nutzen können. Im Folgenden finden Sie einige Möglichkeiten, wie sich diese Integration auf verschiedene Gerätetypen erstreckt:

- Rasche Behebung von Sicherheitslücken
- Nahtlose Rückkehr zur Produktivität
- Verbesserte Mitarbeitererfahrung
- Vertrauen der Mitarbeiter*innen schaffen
- Infrastrukturweite Durchsetzung der Vorschriften
- Stärkere Anpassung an die Unternehmensrichtlinien
- Umfassende, mehrstufige Sicherheitsprozesse
- Bilaterale App-Verwaltung
- Defense-in-Depth-Strategie, unabhängig vom Eigentumsmodell
- Flexible und dennoch robuste Sicherheits- und Verwaltungslösungen, die zusammenarbeiten und umfassende Unterstützung bieten

Mobile Compliance

Die Einhaltung von Vorschriften ist nicht auf regulierte Branchen beschränkt. Für Organisationen in Bereichen wie Finanzen, Gesundheitswesen und Bildung ist sie unerlässlich. Sie umfasst aber auch die Einhaltung von Regeln und Richtlinien, die innerhalb einer Organisation festgelegt wurden, um die speziellen Geschäftsanforderungen zu erfüllen und gleichzeitig die Risiken für die Geschäftskontinuität zu minimieren. In Anbetracht dessen spielt die Implementierung und Durchsetzung einer unternehmensweiten Richtlinie für mobile Geräte, ähnlich wie bei der heutigen Handhabung von Mac Geräten, eine zentrale Rolle bei der Einführung einer umfassenden Strategie für die mobile Sicherheit in Ihrem Gerätepark.

Nehmen wir dieses Beispiel: Mobile Geräte sind in hybriden und dezentralen Arbeitsszenarien einem erhöhten Risiko von Diebstahl, Verlust oder Kompromittierung ausgesetzt, wodurch sensible Unternehmensdaten gefährdet werden können. Die IT-Abteilung kann Verschlüsselungsstandards und sichere Authentifizierungsprotokolle für Geräte und Benutzer*innen durchsetzen, indem sie einen MDM-Workflow zur Bereitstellung standardisierter Sicherheitskonfigurationen nutzt. Darüber hinaus können mit der Fernlöschfunktion bei Bedarf Daten sicher von den betroffenen Geräten gelöscht werden.

Unternehmen können einen Compliance-Plan für mobile Benutzer*innen entwickeln, der auf einem bestehenden Mac Compliance-Plan aufbaut. Dieser Ansatz geht auf inhärente Risiken ein und bietet gleichzeitig eine solide Grundlage, auf der man aufbauen kann. Dies ist besonders wertvoll, wenn es darum geht, Risiken zu mindern, die mit neuen Paradigmen verbunden sind, wie z. B. neu entwickelte mobile Apps im Vergleich zu einer ausgereiften Website, die bereits mit Vorschriften wie dem California Consumer Privacy Act (CCPA) konform ist.

Darüber hinaus geht es bei der Einhaltung von Vorschriften darum, Probleme zu entschärfen und zu erkennen, bevor sie sich zu kritischen Schwachstellen oder Verstößen gegen Vorschriften auswachsen. Hier arbeitet die Kombination aus Sicherheit (Überwachung) und Verwaltung (Durchsetzung) zusammen, um Bedrohungen zu erkennen und zu entschärfen und sicherzustellen, dass mobile Geräte die Vorschriften einhalten.

Angesichts der Vielseitigkeit mobiler Geräte kann es vorkommen, dass Nutzer*innen versehentlich zugelassene Dienste für private Aufgaben oder nicht zugelassene Apps für geschäftsbezogene Aufgaben verwenden. Beide Szenarien bergen Risiken, wie z. B. die Vermischung von Daten, die Beeinträchtigung der Privatsphäre der Benutzer*innen oder die Gefährdung des Unternehmens durch Datenschutzverletzungen und Verstöße gegen Vorschriften.

Wenn Unternehmen die Einhaltung von Richtlinien für mobile Geräte mit der gleichen Ernsthaftigkeit behandeln wie die Einhaltung von Mac Richtlinien, können sie ihre mobilen Endpoints vor den neuesten Bedrohungen schützen und genaue Aufzeichnungen über den Gerätebestand, die Nutzung, die ausgegebenen Geräte, den Zugriff der Mitarbeiter*innen auf Unternehmensdaten und die implementierten Sicherheitsmaßnahmen führen - genau wie bei Mac.

Ein letzter Aspekt bei der Einhaltung der Vorschriften für mobile Geräte ist die laufende Schulung der Benutzer*innen in Sachen Sicherheit. Dieser Aspekt, der oft übersehen wird, aber für einen umfassenden Plan für mobile Sicherheit unerlässlich ist, vermittelt den Nutzer*innen Kenntnisse über bewährte Sicherheitspraktiken, sichere Arbeitsabläufe und Verfahren, die bei potenziellen Sicherheitsbedrohungen zu befolgen sind. Diese Ausbildung ist eine wichtige Schutzmaßnahme, die die Verwaltungs- und technischen Sicherheitsmaßnahmen ergänzt.

Einfach ausgedrückt: Cybersicherheit liegt nicht nur in der Verantwortung der IT-Abteilung oder des Unternehmens - sie liegt in der Verantwortung aller.

Schlüssel zur Vereinheitlichung der Verwaltung und Sicherheit von Mobilgeräten und Macs

Falls es noch nicht klar ist, lassen Sie es uns klar sagen: Der Schlüssel zur Sicherheit ist die Vereinheitlichung von Verwaltung und Sicherheit für Ihre gesamte Flotte.

1. Konvergenz:
Der Erfolg stellt sich ein, wenn Verwaltung und Sicherheit nahtlos mit robusten Sicherheitsprotokollen in einem modernen, mobilzentrierten Arbeitsbereich integriert werden.

2. Überwindung:
Die Überwindung mobiler Sicherheitsprobleme erfordert eine umfassende Lösung im Gegensatz zu den traditionellen Einzelansätzen, bei denen mehrere Tools zusammengefügt werden, ohne dass sich ein einzelnes Tool als besonders effektiv erweist.

3. Konsistenz:
Zur Sicherstellung der Einheitlichkeit gehört die Messung der Sicherheitsgrundlagen auf allen Geräten und die proaktive Überwachung der Endpoints auf Veränderungen, die auf das Vorhandensein von Problemen hindeuten könnten, und ob Sicherheitsbedrohungen, Schwachstellen oder Anomalien untersucht werden müssen.

4. Benutzerfreundlichkeit:
Die Priorisierung der Benutzerfreundlichkeit und deren Abstimmung mit dem Schutz ist ein wesentlicher Bestandteil einer umfassenden Strategie, die das empfindliche Gleichgewicht zwischen Effektivität und Einfachheit für IT, Sicherheitsteams und Endbenutzer*innen betont.

5. Reaktion:
Eine schnelle Reaktion auf Sicherheitsbedrohungen ist unabdingbar, wobei der Schwerpunkt auf der Priorisierung, Untersuchung und Lösung liegt, die alle Gerätetypen, verschiedene Plattformen und die gesamte Infrastruktur umfasst.

6. Gleichgewicht: Das richtige Gleichgewicht zu finden bedeutet, Sicherheit zu erreichen, ohne das Nutzererlebnis zu beeinträchtigen, und die Möglichkeit zu bekräftigen, Sicherheit und Nutzerzufriedenheit nahtlos miteinander zu verbinden.

Wir stellen uns eine Zukunft vor, in der jedes Gerät kompromisslosen Schutz genießt, ohne Kompromisse eingehen zu müssen. Diese Vision stellt das ultimative Ziel dar: unternehmenssichere, benutzerfreundliche Technologie, die von Endbenutzer*innen geschätzt wird und auf die Unternehmen vertrauen. Unsere Vision ist eine nahtlose Verwaltung und ein nahtloser Schutz in jedem Kontext. Wir nennen es **Trusted Access.**

Lassen Sie sich von Jamf dabei helfen, den Sicherheitsbedarf Ihres Unternehmens zu ermitteln und herauszufinden, wie Sie alle Ihre Endpoints verwalten und schützen können.

jamf

www.jamf.com/de/

Los geht's

Oder kontaktieren Sie Ihren bevorzugten Reseller, um Jamf kostenlos zu testen.